January 27, 2017

Unclassified
Cerrid #32125941

MEMORANDUM FOR CHIEF CSE

CSE IM Strategy: Goals for 2017 and Beyond

(For Approval)

Summary

- A CSE Information Management (IM) Strategy was signed in 2012 by the CSE Information Management Senior Official (IMSO), as required by Central Agency at the time. The 2012/13 strategy referenced a five year plan that carried the organization through to FY 2016/17.
- A new CSE IM Strategy has been drafted for FY 2017/18-2019/20, *Enterprise IM Strategy 2017 and Beyond*. This strategy seeks to reinvent, modernize and innovate how the organization manages its information assets. (Reference document: IM Strategy 2016 - 2020.)
- Approval of this strategy by the Chief, CSE is being sought. Government departments are now mandated by Central Agency to have a Deputy-Head approved IM Plan.
- The new IM Strategy was presented to, and endorsed by, the CSE IM/IT Steering Committee on 17 October 2016.

Background

- Treasury Board expectation is that departments will have a Deputy-Head approved IM Plan to demonstrate that IM is integrated as part of organizational business planning and complies with GC horizontal priorities. This requirement is regularly assessed in the Management Accountability Framework (MAF) for IM/IT Stewardship.
- Since the current CSE IM Strategy signed in 2012/13 only carries the organization through to FY 2016/17, a new IM Strategy has been drafted. This strategy sets out

four areas of opportunity which align with CSE overall strategic direction as well as Central Agency priorities[1]. Moreover, the strategy incorporates feedback from focus group discussions with CSE employees as well as the results of an environmental scan of emerging trends for addressing growing IM challenges across industry and government.

- We have identified four key areas of opportunity that will move CSE along the maturity curve from proactive to transformational IM. The four areas of opportunity are as follows:

1. **Mature records & Collections Management** – This involves managing the physical and digital records of the department, identifying possible datasets for release through the Government of Canada's Open Government initiative and ensuring adherence to legislative, Treasury Board and Library and Archives Canada requirements for organizational recordkeeping.
2. **Information Management Compliance** – Establishing a compliance monitoring program to hold the organization accountable for its IM practices is essential to maturing best practices and establishing pro-active measures to address IM accountabilities. A compliance program would reduce our exposure to risk and help the organization meet its legal obligations under the *Access to Information Act* and the *Privacy Act as well as the policy on Management of Government Information.*
3. **Best-In-Class Service Delivery** – Growing and modernizing IM services and better alignment with mission needs was a theme that resonated with focus groups and was proven through a number of pilots conducted with the mission in 2016/17. CSE's IM Advisory Services has resources with over 10 years of experience with enterprise document and records management systems who could play a leadership role in our growing need shared services and shared information in a TS environment; the Library offers a traditional media monitoring service

s.15(1) - DEF

4. **Innovation through Partnership** – This involves experimenting with new ideas like information valuation, engaging partners on challenging projects like building a CSE-wide taxonomy, and finding synergies and economies by sharing knowledge, expertise and products related to open source information discovery.

[1] The GC's horizontal priorities are set out in the Treasury Board GC Enterprise IM Strategy and revised Treasury Board IM policy suite. Central agency is currently reviewing the GC IM vision and strategy with a view to modernizing IM in government. It has four main goals: improving service to Canadians, enabling workforce flexibility & mobility, bringing government closer to citizens and business and supporting innovation and collaboration. At the same time that Central Agency is updating the GC IM vision and strategy, it is also revising the entire IM policy suite. This revision is moving the focus away from basic recordkeeping to treating information as a strategic asset.

- Each area of opportunity includes a number of strategic goals that serve to address business drivers and describe our desired future state. These goals are supported by key activities that identify the specific steps needed to satisfy them. The activities also form the basis for a deliverology schedule that accompanies the strategy as Appendix B.

- The IM Strategy was presented to, and endorsed by, the CSE IM/IT Steering Committee on 17 October 2016. IM/IT Committee October 17 Draft RoD: https://cerrid2.corp.cse/cerrid/llisapi.dll?func=ll&objaction=overview&objid=31795991

Next Steps

CIO will work closely with a communications representative to share strategy highlights and implications with staff.

Recommendation

It is recommended that the Chief approve the CSE *Enterprise IM Strategy 2017 and Beyond*.

A/CIO
IMSO

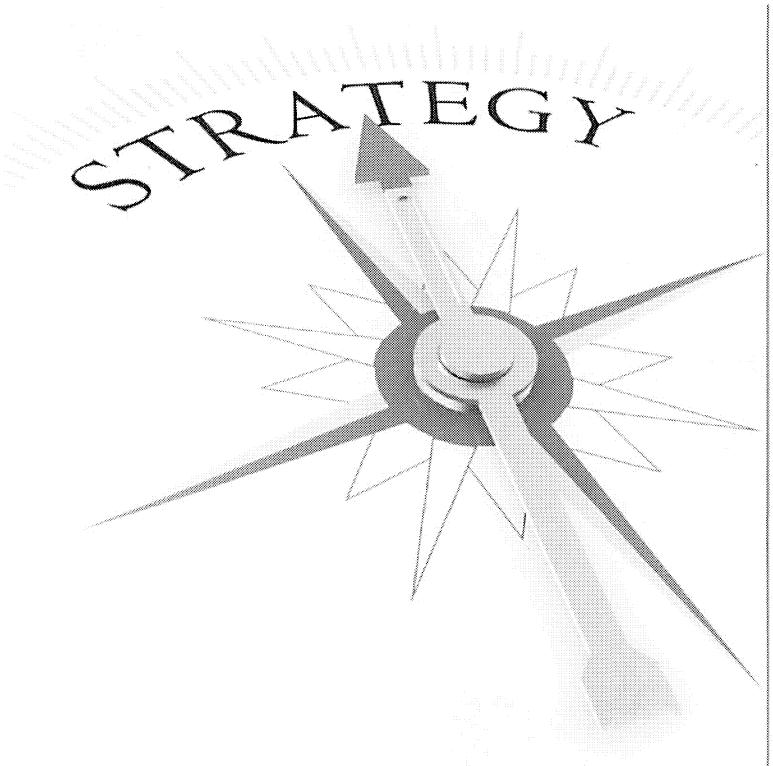
Reviewed by:

Director, Information Management

DELIVERING THE INFORMATION ADVANTAGE

Enterprise Information Management Strategy 2017 and Beyond

Canada



"To manage a business well is to manage its future; and to manage the future is to manage information."

- Marion Harper Jr.

INTRODUCTION

Information, along with people, finances and infrastructure, are key strategic resources in the Government of Canada and is at the very core of CSE's operations. Information is the foundation of everything we do, from service delivery and planning activities to decision-making and policy development.

The quality, reliability and integrity of information are critical to the fulfillment of our mandate, and can only be ensured through enterprise-wide information management (IM). CSE's IM Program supports the delivery of services across the organization for the protection and security of records throughout the lifecycle, while assisting in providing efficient systems for access to the information.

Because of the sensitivity of our information, it is essential that we have the highest IM standards in place. The vast accumulation of information and the added complexity of collaborative ecosystems across the intelligence community, nationally and internationally, create challenges for us. We face a fundamental choice between being in a constant state of catch-up, and opportunity; implicit in this concept is the idea that we are entering a period that requires a transformation in how we manage our information.

The objectives of this enterprise strategy are clear – acknowledge the value of CSE's information, the importance of managing CSE's information at an enterprise level, and the benefits of treating CSE's information as a strategic asset. Every employee is responsible for the success of this strategy – regardless of role, working level, or business line. As CSE employees, we are the stewards of the information we collect and create. It is our duty to safeguard this information as a public trust, and manage it as an asset to maximize its value in the service of Canadians.

WHERE WE ARE TODAY

We are well positioned...

CSE has a mature information management governance structure that provides leadership. This structure is clearly articulated in CSE's policy suite which explains the responsibilities, accountabilities, and expectations of CSE employees in carrying out IM activities. A culture of evidence-based decision making supports good governance by using monitoring and reporting processes as the primary reference for refining existing, and planning new, initiatives.

We have engaged Library and Archives Canada to issue a suite of Records Disposition Authorities that gives us the legal right to dispose of our information. To complement these instruments, we have worked with the business lines to develop records retention and disposition schedules that describe the types of information we have, how long we are required to keep this information, and how we are to dispose of it when the time comes.

Our move from the Confederation Heights Campus to the Edward Drake Building has forced us to reduce our paper footprint and adopt healthy practices to minimize office clutter. Paper reduction goals have also been met through the digitization of paper documents; in fact, CSE was one of the first departments in the Government of Canada to implement such a program.

For the past decade CSE has kept up with the latest Treasury Board-approved Enterprise Content Management (ECM) systems. CERRID ensures standardized electronic document and record management across all business lines. A robust training and awareness program that is dedicated to providing a customized service supports this system through a number of channels, including in-class training, computer-based modules and one-on-one sessions.

During the 2015-2016 Management Accountability Framework (MAF) assessment period, CSE was evaluated on IM and was commended by Treasury Board for its stewardship. CSE completed 100% of planned paper and electronic disposition activities, well above the Government of Canada average, and submitted its departmental Open Government Implementation Plan.

... But not without challenges

While CSE has invested in a designated corporate repository, CERRID, this system does not currently contain and manage all of the organization's unstructured electronic information. CSE stores its information in a number of formats and distributes them across multiple applications and platforms. This practice complicates the search and retrieval process. Moving our holdings into the designated corporate repository will not only help curb the negative effects of information overload, it will better support collaboration and evidence-based decision making.

We know that the volume of information we collect and create is growing at an exponential rate, but are we ready for it. We are creating 150,000 new documents monthly in CERRID alone. Moreover, a recent inventory of our IT infrastructure shows that we have an additional 112 data and information repositories that need to be managed. Although the price of digital storage is on the decline in the real world, CSE could invite additional costs for surpassing storage quotas under its private sector partner agreement. Keeping information longer than we should may also expose the organization to the unnecessary production of stale records in response to Access to Information and Privacy (ATIP) requests, as well as prolonged eDiscovery.

The biggest challenge to achieving the highest level of information management maturity is human. The key to success rests squarely on collaboration, coordination, and cooperation. Employees are also looking for more lightweight systems to perform their work – systems that mirror what they have in their personal lives. We need to strike a balance between traditional time tested practices and newer disciplines that allow information to be handled with more flexibility.

BUSINESS DRIVERS

Although progress has been made on how we manage information, we need to shift toward realizing and sustaining an information advantage for improved business outcomes. The following represents a sample of the business-driven IM requirements that need to be addressed and supported by this strategy.

Driver: Legislated Compliance

Departmental accountabilities, responsibilities and requirements have evolved following the Treasury Board refresh of the IM Policy Suite and Strategy for the Government of Canada, as well as changes to Library and Archives Canada's direction on documentary heritage. CSE will adapt to these changing requirements by ensuring it has the appropriate policies and processes in place.

Driver: Appropriate Collection and Use of Open Source Information Resources

In order to effectively leverage increasing quantities of publicly available information, CSE must assess its current open source information holdings, identify additional information requirements, and ensure appropriate governance of the acquisition, management and use of open source collections. The way in which open source products and services are produced, managed and delivered must undergo a significant transformation. There is a need for innovative, value-added open source products and services that focus on

s.15(1) - DEF

Driver: Diminished Information Risks

Complex organizations like CSE require increasingly sophisticated safeguards to prevent security and privacy breaches. The workforce must understand and apply proper IM practices for sharing and protecting information. It must also exercise its duty to document and its duty to delete. Working in tandem with information security, privacy, litigation and IT specialists, we can begin to develop and implement mitigation measures to reduce risks and improve the integrity of our information.

Driver: Knowledge Gap

The knowledge gap manifests itself on multiple levels, from the individual level all the way to the enterprise level. CSE is facing a wave of impending retirements of long-tenured experts. As each of these valuable resources departs the organization, we need to consider continuity. Moving toward a future where information is used to its fullest potential will require training to aid employees, including IM functional specialists, in acquiring skills for effective IM.

Driver: Data Analytics Imperative

CSE faces increasing demands from across the enterprise for data analytics solutions to address rapidly increasing data volumes. Data literacy will become a core skillset to be embedded throughout the enterprise. The need for data analytics permeates the mission with impacts on foreign intelligence analysis, business intelligence, global situational awareness, and corporate governance. The need to acquire, process, manage and use vast quantities of data, often in real time, will require investment in tools, training and infrastructure; the increased importance of open source data will also require that adequate low side infrastructure be in place in order to effectively extract value from that data.

Driver: Disruptive Business, Service and Technology Trends

Trends in IM present opportunities for change and innovation, and these must be seized. To stay relevant, CSE must reach out to key partners and devote time and money to experimenting with new approaches and technology trends for addressing growing IM challenges.

Driver: Digital Collaboration

To allow for genuine collaboration across the department and the S&I community, CSE needs to reduce information silos, integrate IM practices and automate business processes. CSE must find ways to facilitate knowledge sharing and re-uses of existing information resources. In transitioning to fully digital information collections, CSE must decrease its paper footprint and enable a collaborative environment in which information can be widely accessed. This will involve building and modernizing the Canadian Top Secret Network, and assessing opportunities for shared initiatives to strengthen cooperation and realize efficiencies. For initiatives with IM implications, CSE will have to determine how it manages responsibility for full compliance (i.e. ATIP, IM, records management and legal disclosure obligations being met).

WHERE WE WANT TO BE

Our Vision is to foster an organizational culture where information is safeguarded and managed as a shared strategic asset to advance CSE's cyber mission.

We have identified four key areas of opportunity that will move CSE along the maturity curve from proactive to transformational IM. At the end of our journey, we will be able to declare that:

WE ARE MATURE:

CSE continues to excel at organizational recordkeeping, embraces the move towards greater openness and makes conscious changes in IM practices and investments to improve specific business outcomes.

WE ARE COMPLIANT:

CSE has strengthened policy and legislative compliance and holds the organization accountable for its IM practices.

WE ARE SERVICE-ORIENTED:

CSE offers best-in-class enterprise services to remain relevant from a service offering perspective and also aligned to the objectives of the business.

WE ARE LINKED:

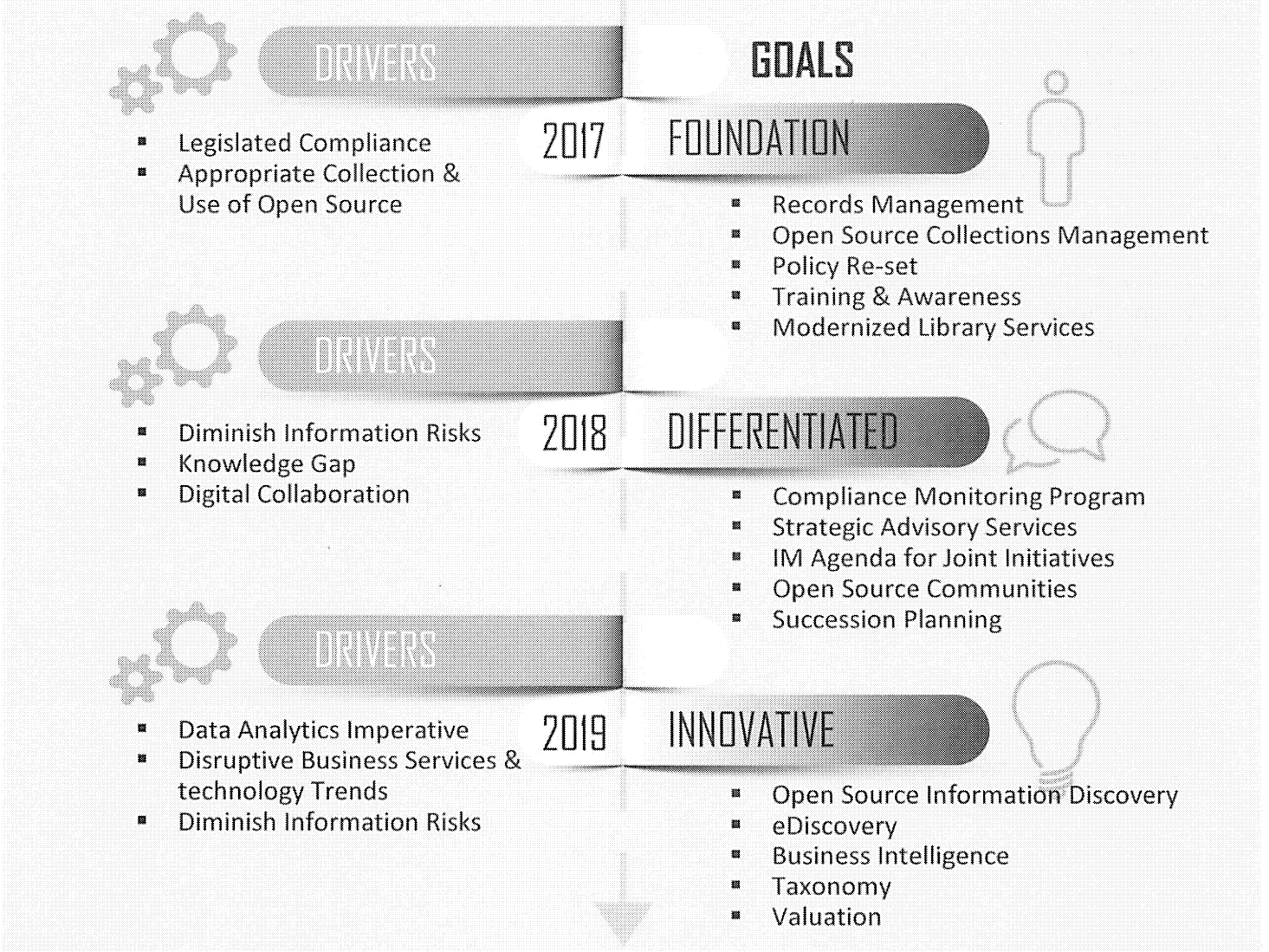
CSE has engaged key partners to transform its capacity, shifting our philosophical outlook of IM and exploiting our information in imaginative ways.

HOW WE WILL GET THERE

Each area of opportunity includes a number of strategic goals that serve to address business drivers and describe our desired future state. These goals are supported by key activities that identify the specific steps needed to satisfy them. The activities also form the basis for an implementation plan that accompanies this strategy.

The timeline below is a high level view of the strategy and how it supports our vision. Goals are categorized by level of complexity:

1. **Foundation** – meeting our essential IM requirements.
2. **Differentiated** – growing our capacity to become more agile with our information.
3. **Innovative** – piloting new ideas to transform our IM posture.



STRATEGIC GOALS

OPPORTUNITY 1: Mature Records & Collections Management

Goal 1: Records Management
Goal 2: Open Source Collections Management

OPPORTUNITY 2: Compliance

Goal 3: Policy Reset
Goal 4: Compliance Monitoring Program
Goal 5: Training & Awareness

OPPORTUNITY 3: Best-In-Class Service Delivery

Goal 6: Strategic Advisory Services
Goal 7: Open Source Information Discovery (OSID)
Goal 8: Modern Library Services
Goal 9: eDiscovery
Goal 10: Business Intelligence

OPPORTUNITY 4: Innovation Through Partnership

Goal 11: IM Agenda for Joint Initiatives
Goal 12: Open Source Communities
Goal 13: Industry & Academia Touchpoints

Appendix A: Mapping to CSE Vision 2020 Strategic Direction

Appendix B: Implementation Plan

OPPORTUNITY 1: Mature Records & Collections Management

WE ARE MATURE

Bringing CSE to a higher level of maturity where policy and legislative requirements are fully met and the department has access to high-quality, authoritative information to support its business goals.

1 : Records Management

Manage the physical and digital records of the department, identifying possible datasets for release through the Government of Canada's Open Government initiative and ensuring adherence to legislative, Treasury Board and Library and Archives Canada requirements for organizational recordkeeping.

KEY ACTIVITIES

- Create an inventory that identifies and contextualizes CSE's information repositories of business value.
- Maximize the release of information in support of the Government's Open Government initiative, subject to valid security and privacy exceptions.
- Identify key areas of risk to CSE's information resources and implement mitigation strategies.
- Increase disposition on structured data in corporate databases.
- Streamline processes for managing and transferring records of archival value.
- Continue digitization initiatives.

2 : Open Source Collections Management

Enhance traditional library services to better align with corporate and mission objectives and to optimize the department's open-source collections.

KEY ACTIVITIES

- Issue a collection development policy that sets out well-defined criteria for inclusion in CSE's open source collections.
- Acquire and sustainably manage commercial electronic resources that are targeted to the various CSE communities.
- Upgrade the library's cataloguing software to enable federated searching across the Tutte Institute for Mathematics and Computing (TIMC) and the corporate library collections.
- Enhance the user interface and promote the broader use of CSE's open source information resources.

OPPORTUNITY 2: Compliance

WE ARE COMPLIANT

Strengthening policy and legislative compliance by implementing renewed policies, performing a monitoring and reporting function, and revamping the training program.

3 : Policy Reset

Create a cohesive IM policy suite to ensure consistency and proper alignment with CSE and Government of Canada direction.

KEY ACTIVITIES

- Review, update and consolidate IM policies.
- Address policy gaps e.g. Open Government obligations, process for departing employees, eDiscovery, Open Source Information Discovery activities, etc.

4 : Compliance Monitoring Program

Establish a compliance monitoring function in IM whereby information systems and settings would be actively monitored for policy compliance.

KEY ACTIVITIES

- Identify theme activities for assessing compliance with Treasury Board and departmental IM policies and follow-up actions for non-compliance.
- Establish governance for the program to include key accountabilities and responsibilities within CSE with respect to the monitoring process as well as reporting requirements.
- Conduct a pilot project involving a chosen business line.

5 : Training & Awareness

Strengthen employee understanding of their individual accountabilities, and drive awareness and change within the culture of the business lines.

KEY ACTIVITIES

- Develop and implement a mandatory IM awareness session for all CSE employees.
- Make better use of IM didactic material available across Government for internal re-use.

OPPORTUNITY 3: Best-In-Class Service Delivery

WE ARE SERVICE-ORIENTED

Reaching new levels of excellence by growing and modernizing existing services and introducing new services.

6 : Strategic Advisory Services

Provide insight and guidance at a strategic level to strengthen internal IM governance and promote CSE's role as a leading expert of Government of Canada IM solutions in the top secret environment.

KEY ACTIVITIES

- Continue conducting digital disposition activities on unstructured data and institutionalize best practices through policy, training & awareness and/or compliance monitoring.
- Enhance CSE's information architecture by ensuring tools, systems and technical solutions implement enterprise IM requirements.
- Pioneer the role of the Data Steward.

7 : Open Source Information Discovery (OSID)

Expand the role of OSID to serve as an S&I community centre of excellence for the analysis, reporting and dissemination of products and services derived from OS information, and to effectively organize the acquisition and management of OS information, resources and tools.

KEY ACTIVITIES

- Assess and acquire a variety of OS tools and data sets.
-
- Develop innovative products and service delivery options.
- Develop OSID tradecraft and techniques.
-

OPPORTUNITY 3: Best-In-Class Service Delivery

WE ARE SERVICE-ORIENTED

Reaching new levels of excellence by growing and modernizing existing services and introducing new services.

8 : Modern Library Services

Connect employees with the Open Source electronic and print information they need to be successful in their work through in-depth research, annotated bibliographies and a modern online presence.

KEY ACTIVITIES

- Implement enhanced processes and/or systems to better gather, track and analyze client requirements for open source research and material.
- Enhance research products by leveraging OSID tools and optimize dissemination platforms.

9 : eDiscovery

Introduce an in-house expertise capable of performing electronic searches across all information systems in support of access to information and litigation requests, which will allow the department to execute discovery consistently and increase the level of quality control.

KEY ACTIVITIES

- Codify the processes for identifying information that must be produced for access to information or litigation purposes.
- Implement a new capability to perform searches across the increasingly complex technology and application infrastructure at CSE.

10 : Business Intelligence (BI)

Develop a modern BI service by creating a holistic approach that leverages technical innovations, data analytics, and user engagement.

KEY ACTIVITIES

- Assess and document existing BI initiatives within CSE.
- Develop a strategic overview of emerging BI trends and standards.
- Explore a proper governance model, innovative analytic solutions, and integrated information management.

OPPORTUNITY 4: Innovation Through Partnership

WE ARE LINKED

Unlocking transformational change by engaging other government departments, 5-Eyes and private sector partners to leverage lessons learned, collaborate on initiatives and keep up-to-date on latest industry trends.

11 : IM Agenda for Joint Initiatives

Engage with CSIS in ongoing bilateral knowledge sharing and work collaboratively with Government of Canada departments that are involved in rolling out shared services to ensure desirable features can be leveraged by CSE as well as OGD's IM and records management programs.

KEY ACTIVITIES

- Continue working with CSIS under the auspices of Integrated Internal Services Working Groups.
- Explore a for OS collections.
- Champion the adoption of and partner with on piloting configurations (e.g. Auto-classification, eDiscovery Rights).
- Participate in other centrally coordinated working groups to influence technical developments related to IM (e.g. MyGCHR).

12 : Open Source Communities

Actively develop a network of national and international partnerships in the Open Source information space.

KEY ACTIVITIES

- Nationally, stand up an active community of interest focused on sharing OS expertise and products by leveraging expertise of . These partners will form the core of a working group.
- Internationally, take advantage of the International Open Source Working Group (IOSWG) to

OPPORTUNITY 4: Innovation Through Partnership

WE ARE LINKED

Unlocking transformational change by engaging other government departments, 5-Eyes and private sector partners to leverage lessons learned, collaborate on initiatives and keep up-to-date on latest industry trends.

13 : Industry & Academia Touchpoints

Partner with industry and academia to keep abreast of the latest trends and thinking and help evolve CSE's IM practices.

KEY ACTIVITIES

- Explore approaches and tools for implementing a CSE taxonomy.
- Explore a sustainable and whole-of-system approach to the valuation of CSE information assets.
- Work with vendors on tools development.
- Develop an academic outreach program for IM/RM succession planning and strategic advancements.

Appendix A: Mapping to CSE Vision 2020 Strategic Direction

IM Strategic Goals	CSE Strategic Direction: Trust and Confidence	A Lead Authority in Cyber Security	Premier Services in Cyber Operations	Enterprise Service Provider for the S&I Community
Records Management	✓			
Open Source Collections Management		✓	✓	
Policy Reset	✓			✓
Compliance Monitoring Program	✓			✓
Training & Awareness	✓			✓
Strategic Advisory Services			✓	✓
Open Source Information Discovery (OSID)		✓	✓	
Modern Library Services		✓	✓	
eDiscovery	✓			
Business Intelligence	✓		✓	
IM Agenda for Joint Initiatives				✓
Open Source Communities		✓	✓	
Industry & Academia Touchpoints	✓			✓

Appendix B-1a: Implementation Plan

Mature Records & Collections Management - Records Management

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Create an inventory that identifies and contextualizes CSE's information of business value.	▪ CSE has an inventory that enables sound decision making, services, ongoing reporting and answers performance and accountability requirements.	▪ Increased use of the inventory across the organization.
▪ Maximize the release of information in support of the Government's Open Government initiative, subject to valid security and privacy exceptions.	▪ A drive for openness that is embedded in CSE culture and processes. ▪ CSE contributes to the Open Data Dialogue through the release of data sets and transfers of information resources of enduring value (IREV).	▪ Inventory of data and information resources of business value is complete and current. ▪ Public releases of CSE datasets and information resources on open.canada.ca increase yearly in accordance with TBS direction. ▪ CSE has maximized the removal of access restrictions on departmental IREV prior to transfer to LAC.
▪ Identify key areas of risk to CSE's information resources and implement mitigation strategies.	▪ Information that is essential to running our business is available in the face of physical or technological disaster. ▪ There is an established risk register for identifying risks to information resources and creating risk profiles specific to IRBVs. ▪ Personal information is retained and disposed of to meet *Privacy Act* and Access to Information and Privacy (ATIP) requirements. ▪ Appropriate use of system access permissions and classification.	▪ Essential records are identified and protected. ▪ Inappropriate or inadvertent information disclosures or loss incidents are minimized.
▪ Increase disposition on structured data in corporate databases.	▪ Increase in accountability to TBS and LAC on the disposition of corporate information. ▪ ATIP and litigation risks diminish.	▪ Automated disposition capabilities are included in new systems.
▪ Streamline processes for managing and transferring records of archival value.	▪ LAC policy requirements for documentary heritage are met. ▪ Records disposition authorities (RDAs) are current. ▪ CSE manages born-digital information.	▪ Declassification/downgrading program and/or policies are established. ▪ Current RDAs are updated and integrating into a single document. ▪ CSE has implemented a formal program to manage born-digital information.
▪ Continue digitization initiatives.	▪ Reduce our physical footprint and modernize processes. ▪ Increased searchability of information holdings.	▪ Physical space occupied decreases. ▪ Reduced search time for information retrieval.

Appendix B-1b: Implementation Plan

Mature Records & Collections Management - Open Source Collections Management

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Issue a collection development policy that sets out well-defined criteria for inclusion in CSE's open source collections.	▪ CSE has an open source collection that precisely links to CSEs mandates.	▪ Loans as a percentage of the collection increase by 20%.
▪ Acquire and sustainably manage commercial electronic resources that are targeted to the various CSE communities.	▪ Funds are accountably spent and budget has flexibility embedded. The value for dollars for the collection is made apparent.	▪ Usage metrics for the commercial resources is monitored and all seats are in use.
▪ Upgrade the library's cataloguing software to enable federated searching across the TIMC and the corporate library collections.	▪ Both CSE library catalogues can be searched in one place.	▪ Number of library requests that originate in the catalogue increase by 15%.
▪ Enhance the user interface and promote the broader use of CSE's open source information resources.	▪ Information resources for the enterprise are easy to find, use and share.	▪ Every resource sees an increase in page views.

Appendix B-2: Implementation Plan

Compliance – Policy Reset

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Review, update and consolidate IM policies.	▪ Consistent management of CSE information.	▪ Targeted IM behaviour improves by 10%.
▪ Address policy gaps e.g. Open Government obligations, process for departing employees, eDiscovery, Open Source Information Discovery activities, etc.	▪ All IM requirements are covered by policy.	▪ Annual policy gap analysis shows diminished gaps from previous year.

Compliance – Compliance Monitoring Program

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Identify theme activities for assessing compliance with Treasury Board and departmental IM policies and follow-up actions for non-compliance.	▪ Compliance plan that identifies theme activities.	▪ Plan complete and in place by target date. ▪ With plan complete, able to move to the next step, governance.
▪ Establish governance for the program to include key accountabilities and responsibilities within CSE with respect to the auditing and monitoring processes as well as reporting requirements.	▪ Governance model is in place.	▪ Policy instrument issued and promulgated to support IM monitoring and reporting.
▪ Conduct a pilot project with a chosen business line.	▪ A business line is subject to monitoring of one theme activity for a six month period.	▪ Reporting results in behavioural change.

Compliance – Training & Awareness

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Develop and implement a mandatory IM awareness session for all CSE employees.	▪ Employees are informed of their IM responsibilities.	▪ Percentage of employees trained achieves and stays over 90%.
▪ Make better use of IM didactic material available across Government for internal re-use.	▪ CSE spends less time creating material and reuses what is available from OGDs.	▪ Percentage of new versus reused material. Reused material exceeds 50%.

Appendix B-3a: Implementation Plan

Best-In-Class Service Delivery – Strategic Advisory Services

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Continue conducting digital disposition activities on unstructured data and institutionalize best practices through policy, training & awareness and/or compliance monitoring.	▪ CSE employees perform their information lifecycle duties delegated to them from the *Policy on Information Management.*	▪ Increase of finalized documents within the corporate repository.
▪ Enhance CSE's information architecture by ensuring tools, systems and technical solutions implement enterprise IM requirements.	▪ Information management is integrated into tools, systems and technical solutions. ▪ Principles of reuse and information authority are adhered to.	▪ All new business requirements documentation includes information management requirements as identified by TBS for the IRBV inventory.
▪ Pioneer the role of the Data Steward.	▪ Improved IM across the organization. ▪ Data Stewards deliver tailored service to meet specific client needs.	▪ Reduction in HPSM tickets requesting IM assistance.

Best-In-Class Service Delivery – Open Source Information Discovery (OSID)

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Assess and acquire a variety of OS tools and data sets.	▪ An inventory of robust analytic tools and a wide range of open source information resources are in place.	▪ Tools are assessed against a set of established performance criteria. ▪ At least two analytic tools are procured and in use by target date.
▪ Develop innovative products and service delivery options.	▪ Reporting available in multiple formats across different platforms.	▪ Three kinds of reporting templates in active use: Ongoing Topic Briefs, and Deep Dive Research Papers. ▪ Products available via an OSID dedicated portal and at least one other delivery method. Some products
▪ Develop OSID tradecraft and techniques.	▪ OSID team is a center of analytic excellence for open source information acquisition, collation, synthesis, analysis and dissemination tradecraft.	▪ An OSID Analyst's Handbook is produced and kept up to date with analytic tradecraft, training tips and best practices.

Appendix B-3b: Implementation Plan

Best-In-Class Service Delivery – Modern Library Services

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Implement enhanced processes and/or systems to better gather, track and analyze client requirements for open source research and material.	▪ The library is familiar with their clients and monitors all requests. ▪ Management is made aware of the requests being completed.	▪ Monthly metric reports on client requests completed.
▪ Enhance research products by leveraging OSID tools and optimize dissemination platforms.	▪ The library's products are improved, promoted and at the fingertips of analysts.	▪ Products viewed 20% more.

Best-In-Class Service Delivery – eDiscovery

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Codify the processes for identifying information that must be produced for access to information or litigation purposes.	▪ Appropriate information is produced with consistency, security and confidentiality.	▪ Reduced resources and time spent in eDiscovery. ▪ CSE processes are consistent and auditable.
▪ Implement a new capability to perform searches across the increasingly complex technology and application infrastructure at CSE.	▪ Legally defensible and auditable controls are in place.	▪ Legal hold capability exists across the enterprise. ▪ Ability to collect forensics evidence and demonstrate compliance.

Best-In-Class Service Delivery – Business Intelligence

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Assess and document existing BI initiatives within CSE.	▪ A broad understanding of BI activities across the enterprise.	▪ A consolidated report detailing all current and currently proposed BI initiatives is produced.
▪ Develop a strategic overview of emerging BI trends and standards.	▪ Ability to assess the level of BI maturity across CSE.	▪ A report on BI standards is produced, complete with recommendations for implementation.
▪ Explore a proper governance model, innovative analytic solutions, and integrated information management.	▪ Foundational strategy in place for the implementation of enterprise-wide BI.	▪ A comprehensive BI strategy prepared and presented to IM/IT SC.

Appendix B-4a: Implementation Plan

Innovation Through Partnership – IM Agenda for Joint Initiatives

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Continue working with CSIS under the auspices of Integrated Internal Services Working Groups.	▪ Opportunities are assessed and implemented to strengthen cooperation, collaboration and realize efficiencies.	▪ A detailed analysis (i.e. value proposition, impact and implementation) and recommendations on IM-related potential shared service initiatives, such as RM, data management, archival services, library services, etc. is completed.
▪ Explore a for OS collections.	▪ CSE and CSIS have a joint vision for OS collections.	▪ An options analysis for the of OS collections is complete and a decision reached.
▪ Champion the adoption of and partner with on piloting configurations (e.g. Auto-classification, eDiscovery Rights).	▪ A strong partnership with aligns our platforms for a common approach.	▪ Evaluation of capabilities. ▪ Quarterly meetings with on specific agenda items.
▪ Participate in other centrally coordinated working groups to influence technical developments related to IM (e.g. MyGCHR).	▪ IM Requirements are built into new applications.	▪ Regular meetings with relevant stakeholders.

Innovation Through Partnership – Open Source Communities

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Nationally, stand up an active community of interest focused on sharing OS expertise and products by leveraging expertise of These partners will form the core of a working group.	▪ Closer collaboration between agencies.	▪ The COI meets at least twice a year.
▪ Internationally, take advantage of the International Open Source Working Group (IOSWG) to	▪ Analytic knowledge transfer and increased CSE capabilities.	▪ Increased contributions of CSE products to ▪ Team members make presentations to both IOSWG events every year. ▪ An international integree is embedded within the OSID team for at least six months.

Appendix B-4b: Implementation Plan

Innovation Through Partnership – Industry & Academia Touchpoints

KEY ACTIVITY	OUTCOME	PERFORMANCE INDICATOR
▪ Explore approaches and tools for implementing a CSE taxonomy.	▪ Recommendation on a CSE taxonomy.	▪ Development of white paper is monitored.
▪ Explore a sustainable and whole-of-system approach to the valuation of CSE information assets.	▪ A valuation approach that allows CSE to categorize its information assets, potentially reduce inventory carry costs, and help prioritize and budget IT/business initiatives.	▪ A proposed method of measuring information quality and value characteristics. ▪ A process for performing, reviewing, and communicating information asset valuation assessments.
▪ Work with vendors on tools development.	▪ Vendors have implemented desired features.	▪ The team identifies at least two opportunities for tool development, such as improved auditing function in analytic tools, and works directly with the vendor to enhance capabilities.
▪ Develop an academic outreach program for IM/RM succession planning and strategic advancements.	▪ IM succession planning and strategic advancements is improved.	▪ Biannual meetings with academic partners.

Recommended by:

Date:

Director, Information Management (CIO-E)

Endorsed by:

Date:

Acting Deputy Chief - Chief Information Officer (CIO)
Information Management Senior Official (IMSO)

Approved by:

Date: FEB 06 2017

Greta Bossenmaier
Chief, Communications Security Establishment

SECRET
CERRID# 33115963
ECT# 17-26249

4 January 2017

MEMORANDUM TO THE MINISTER OF NATIONAL DEFENCE

Notification of Cyber Defence Activities

(For Information)

- This Memorandum is to inform you that, at the request of CSE will conduct on-going cyber defence on the computer systems and networks under the control and supervision of and by extension

- To prevent and respond to compromises to Government of Canada networks and information technology infrastructure, CSE deploys its cyber defence mitigation tools to the computers and networks of requesting departments and agencies. These cyber defence activities help to inform and protect the Government of Canada from sophisticated cyber threats.

- Under the terms of CSE's *Ministerial Authorization on Cyber Defence Activities,* CSE is required to inform you when it accepts a request from a federal institution to conduct cyber defence activities under the authority of this MA.

- Attached for your information is a copy of the letter of request from CSE's letter of response, and the current list of federal institutions where CSE conducts ongoing cyber defence activities.

- Should you have any questions, please do not hesitate to let me know.

Greta Bossenmaier
Chief

Canada

UNCLASSIFIED

September 13th, 2016

Scott Jones
Deputy Chief Information Technology Security
Communications Security Establishment
PO Box 9703 Terminal
Ottawa, ON, K1G 3Z4

Dear Mr. Jones,

This is a request for the Communications Security Establishment (CSE) to conduct on-going cyber defence activities to help protect the computer systems and networks under the control and supervision of Activities may include, but are not limited to, computer and network monitoring, related analysis, and the provision of mitigation services.

As Chief Information Officer and Departmental Security Officer, we have the authority to provide CSE with access to the computer systems and networks under the control and supervision It is understood that if, during the course of CSE's cyber defence activities, private communications could be intercepted, an Authorization from the Minister of National Defence must first be in effect.

It is acknowledged that data obtained by CSE during the course of cyber defence activities will be considered to be under CSE control if it is relevant (or in the case of private communications, essential) to CSE's mandate as stated in 273.64(1)(b) of the *National Defence Act*. That data may be used for the purpose of fulfilling that mandate, and may be shared with domestic and international partners involved with cyber security, both in the public and private sector. Data that is not relevant to CSE's mandate must be deleted in accordance with CSE's retention schedules.

We authorize direct liaison between and CSE in order to develop the scope of cyber defence activities. We will be the primary points of contact for

It is understood that CSE activities are subject to review by the CSE Commissioner, the Information Commissioner, the Privacy Commissioner, the Auditor General and any other body established by Parliament for review purposes. Interviews or documentation may be requested as part of a review; will cooperate fully with any such requests.

Canada

s.15(1) - DEF

s.16(2)(c)

UNCLASSIFIED

It is understood that at any time, or CSE may terminate any or all cyber defence activities conducted by CSE on computer systems and networks.

Sincerely,

Chief Information Officer

Departmental Security Officer

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

UNCLASSIFIED

P.O. Box 9703
Terminal
Ottawa, Canada
K1G 3Z4

C.P. 9703
Terminus
Ottawa, Canada
K1G 3Z4

Our file Notre référence
 # 2954219

DEC 2 8 2016

Chief Information Officer

Dear

The Communications Security Establishment (CSE) thanks you for your request to have CSE conduct cyber defence activities to help protect the computer systems and networks under the control and supervision of CSE looks forward to providing our service to your department.

Representatives from the CSE Cyber Defence team will work with your department to clarify the details surrounding the specific services to be provided. All cyber defence services conducted by CSE will be done in accordance with 273.64(1)(b) of the *National Defence Act* and CSE's internal policies.

Please do not hesitate to contact us for further discussions regarding CSE's Cyber Security Services. At this time, your CSE point of contact is Director Cyber Defence Operations.

Regards,

Scott Jones
Assistant Deputy Minister, IT Security

Canada

Ongoing Cyber Defence Activities

Under the current Ministerial Authorization, "Communications Security Establishment Cyber Defence Activities," effective 31 May 2016, CSE is engaged in ongoing cyber defence activities (that risk interception of private communications) in support of the computer systems and networks under the control and supervision of the following federal institutions:

Communications Security Establishment;
Department of National Defence;

Global Affairs Canada;

Shared Services Canada (including federal institutions using internet access consolidation points administered by Shared Services Canada);

- CSE intends to continue these cyber defence activities with these federal institutions under the 2017-2018 Ministerial Authorization.

- All cyber defence activities carried out on the computer systems and networks of federal institutions are conducted under the strict supervision of CSE personnel in cooperation with the requesting federal institution's staff, and in accordance with established policies and procedures.

TOP SECRET//SI//CEO
Cerrid # 33204488
ECT # 17-26286

CSE – CSIS Update to the National Security Advisor

(For Approval)

Summary

- Attached for your signature is a letter to the National Security Advisor, developed jointly by CSE and CSIS, to provide an update on the ongoing collaborative work between our two agencies.
- The letter has been approved at the ADM level at both agencies.
- Upon your signature, the letter will be provided to Director Coulombe for signature and then provided to the NSA.

Dominic Rochon
Deputy Chief, Policy and Communications

TOP SECRET//SI//CEO

CCM #: 25675 CERRID #: 31292832

MEMORANDUM TO THE NATIONAL SECURITY ADVISOR

CSE-CSIS COLLABORATION

ISSUE:

To provide an overview of current priority areas of collaboration between the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE).

BACKGROUND:

CSIS and CSE have common national security goals and share a number of challenges in keeping Canada, Canadians and Canadian interests safe and secure. The two agencies continue to work collaboratively in accordance with our respective mandates and legislative authorities to effectively fulfill the government's national security intelligence requirements.

The CSE-CSIS Joint Management Team (JMT) – a group comprised of members of both Executive Committees – is the agencies' senior forum for setting priority activities for cooperation and addressing issues of mutual interest. The JMT is supported by four ADM-level sub-groups that meet as required, specifically the Operational, Cyber, Corporate, and Integrated Internal Services JMT Pillars.

AREAS OF COLLABORATION:

Operational Pillar

CSIS and CSE have recently set strategic directions to lead them through the next five years, and are well aligned to with common priorities in and shared services. Over recent months, CSE has

The passage of Bills C-44 and C-51 has required an evolution of the agencies' policy instruments and work continues on the implementation of these changes. Bill C-44 has allowed CSE to support CSIS more effectively in the pursuit of Canadian targets, predominantly outside Canada. At present, CSE is providing assistance on

Bill C-51 has opened a new area of collaboration between the agencies – threat reduction – and a Memorandum of Understanding was signed in June 2016 to guide this collaboration.

The agencies continue to mature collaboration

CSE and CSIS have been working together on advancing relations with designated partners

In addition to the above, there are other established areas of collaboration and personnel exchange. For example,

Collaborative work is underway to to reduce the likelihood of duplication.

Other areas of collaboration include

In addition, through standing requests for assistance, CSIS takes advantage of CSE's technical capabilities

Cyber Pillar

The agencies created a distinct Pillar for cyber to reflect the importance placed on cyber issues and ensure they are addressed on a regular basis.

The agencies have also developed a governance structure

Moving forward, CSIS and CSE will prioritize cyber engagement

We are also enhancing collaboration in the

Corporate Pillar

Corporate collaboration between CSIS and CSE spans the policy, communications, finance, human resources,
and these counterparts meet regularly. Domestically, we collaborated closely

The agencies are also currently

Moving forward, we plan to coordinate on how to best support the National Security and Intelligence Committee of Parliamentarians, and to implement any policy, legal, or operational changes required as a result of possible amendments to Bill C-51.

Internationally, the agencies coordinated on travel to Five Eyes countries, namely to attend and deliver joint remarks at the meeting that took place and to meet with our partners to discuss multi-agency collaboration. Recently, we also jointly hosted a CIO forum which proved to be very successful.

Being co-located continues to benefit the agencies' relationship-building and cultural awareness efforts. We frequently extend invitations for events and host joint CSE-CSIS gatherings such as GCWCC events and an annual CSE-CSIS volleyball tournament. Our proximity also encourages collaboration on internal communications, for example our recent communication and we liaise on public communications such as our respective Twitter accounts.

Integrated Internal Services Pillar

Integrated Internal Services (IIS) is an initiative that was launched in March 2016 that will allow CSE and CSIS to become more resilient within a joint community by leveraging best practices for internal services and building on each other's strengths. Co-location has seen areas for collaboration naturally arise, to official languages, Further, the agencies have begun 12-month pilots in the materiel management, and finance domains, during which a small number of participating employees are moving from one organization to the other, providing services to both.

A second wave of pilots to begin this year will cover further areas within finance, as well as areas in procurement, emergency management, and communications. One specific example of

an IIS initiative is the plan to shift to a single Enterprise Resource Planning System to support financial and Asset management at both agencies, which will replace some of our financial, procurement and asset management legacy applications.

We trust that you will find this overview of our collaboration to be a helpful contribution. As always, please do not hesitate to contact us should you require further information.

Greta Bossenmaier
Chief, CSE

Michel Coulombe
Director, CSIS

FEV FEB 0 3 2017

SECRET//SI//CEO
Cerrid # 32564000

BRIEFING NOTE FOR THE MINISTER OF NATIONAL DEFENCE

Response to the CSE Commissioner's *Spring 2016 "Spot check" Review of CSE Use and Retention of Foreign Signals Intelligence One-end Canadian Communications*

(For Action)

Summary

- You received a letter from the CSE Commissioner, dated 5 December 2016, providing the results of his latest *Spot Check Review of CSE Use and Retention of Foreign Signals Intelligence One-end Canadian Communications.*
-
-

Background

- The CSE Commissioner conducted this review to verify the effectiveness of CSE's procedures regarding the use, retention and deletion of recognized SIGINT one-end Canadian communications acquired by CSE, including those from its Second Party partners. Those procedures demonstrate CSE's compliance with legal requirements to only retain and use one-end Canadian communications that are essential to international affairs, defence or security.

- While previous spot check reviews have focused only on recognized Private Communications (PCs) incidentally acquired by CSE in its activities under Ministerial Authorization (MA),

- The Commissioner's office examined records related to SIGINT communication events collected by CSE and its Second Party partners that were recognized by CSE analysts during the period of 1 March 2016 to 31 May 2016. This included communications used in reports, retained for future use, as well as those deemed to have no Foreign Intelligence (FI) value. intelligence reports were produced based on one-end Canadian communications during the review period.

Considerations

- The CSE Commissioner was satisfied that:
  -
  -
  -
-
-

Next Steps

- I have enclosed, for your consideration, a draft letter of response to the CSE Commissioner.

Greta Bossenmaier
Chief

Communications Security Establishment Commissioner

The Honourable Jean - Pierre Plouffe, C.D.

Commissaire du Centre de la sécurité des télécommunications

L'honorable Jean - Pierre Plouffe, C.D.

TOP SECRET//SI//CEO

Our file # 2200–107

December 5, 2016

The Honourable Harjit S. Sajjan, PC, OMM, MSM, CD, MP
Minister of National Defence
101 Colonel By Drive
Ottawa, ON K1A 0K2

Subject: Review of CSE Use and Retention of Foreign Signals Intelligence One-end Canadian Communications

Dear Minister:

The purpose of this letter is to provide you with the results of a spot check review of recognized one-end Canadian communications related to foreign signals intelligence (SIGINT) collection that the Communications Security Establishment (CSE) used, retained or deleted during the period of March 1, 2016, to May 31, 2016. One-end Canadian communications are those where one of the communicants is either physically located in Canada — that is, a private communication (PC) — or where one communicant is a Canadian physically located outside Canada. To verify that CSE does not target Canadians and effectively applies satisfactory measures to protect Canadians' privacy, I examined a sample of one-end Canadian communications acquired by CSE, including from its second party partners in the United States, the United Kingdom, Australia and New Zealand.

The review was conducted under the Commissioner's general authority set out in paragraph 273.63(2)(*a*) of the *National Defence Act* (NDA) and the authority set out in subsection 273.65(8) of the NDA to determine whether activities carried out under a ministerial authorization (MA) are authorized by the Minister of National Defence. CSE had no warning that the office was about to conduct the spot check.

Subsection 273.65(1) of the NDA permits the Minister to authorize CSE in writing — for the sole purpose of obtaining foreign intelligence (FI) and only after the Minister is satisfied that specific conditions set out in subsection 273.65(2) of the NDA have been met — to intercept PCs in relation to an activity or class of activities specified in an MA. The MAs set out the formal framework for dealing with PCs that have been intercepted unintentionally through SIGINT activities and shield CSE from the prohibition respecting the interception of PCs found in Part VI of the *Criminal Code*. Currently, CSE conducts three distinct SIGINT collection activities or classes of activities under MAs: (1) collection activities; (2) collection activities; and (3) collection activities.

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
T: 613-992-3044 F: 613-992-4096

To support the Minister in his accountability and control of CSE, the MAs require CSE to report to the Minister — after the MAs expire (no MA may be in effect for longer than one year) — information relating to the privacy of Canadians, including the number of recognized PCs unintentionally intercepted pursuant to the MAs that are used or retained on the basis that they are essential to international affairs, defence or security.

If a CSE analyst whose function is directly related to the production of FI reports recognizes that an intercepted communication is one-end Canadian — whether the communication is acquired by CSE or collected by a Second Party — then the analyst must, upon recognition, annotate the communication (that is, indicate that the communication is one-end Canadian and whether it is to be retained, due to its FI value, or deleted).

One-end Canadian communications used in FI reports are retained by CSE. One-end Canadian communications (and communications containing information about Canadians) that are not essential to international affairs, defence or security must be annotated for deletion and are automatically removed from the repository

If a one-end Canadian communication is deemed essential by an analyst and it is annotated for retention but not used in an FI report within the repository automatically annotates it for deletion. At that time, the analyst who had originally marked the communication as essential is prompted by the system to re-assess whether it remains essential, and, if so, to re-annotate it for retention. (Note that

Based on the information reviewed and the interviews conducted,

-
-
-

Over the years, CSE has enhanced its operational and administrative processes and technical systems relating to one-end Canadian communications,

Before this this letter was finalized, CSE officials had an opportunity to review it for factual accuracy and to comment on the findings.

If you have any questions or comments, I will be pleased to discuss them with you at your convenience.

Yours sincerely,

Jean-Pierre Plouffe

cc: Ms. Greta Bossenmaier, Chief, CSE

Minister
of National Defence

Ministre
de la Défense nationale

Ottawa, Canada K1A 0K2

SECRET

CERRID # 32564165

FEV
FEB 21 2017

The Honourable Jean-Pierre Plouffe
Communications Security Establishment Commissioner
90 Sparks Street, Suite 730
P.O. Box 1984, Station B
Ottawa, Ontario
K1P 5B4

Dear Commissioner Plouffe:

I am writing to respond to your letter dated 5 December 2016, related to your *Spot Check Review of CSE Use and Retention of Foreign Signals Intelligence One-end Canadian Communications*.

I look forward to receiving future reports resulting from your continued commitment to conduct reviews on CSE use and retention of one-end Canadian communications.

Sincerely,

The Hon. Harjit S. Sajjan, PC, OMM, MSM, CD, MP

cc: Greta Bossenmaier, Chief, CSE

Canada

FEV FEB 0 1 2017

TOP SECRET//SI//CEO
Cerrid # 32826222

BRIEFING NOTE FOR THE MINISTER OF NATIONAL DEFENCE

Response to the CSE Commissioner's *Review of CSE Cyber Defence Metadata Activities*

(For Action)

Summary

- You received a letter from the CSE Commissioner, dated 5 December 2016, providing the results of his *Review of CSE Cyber Defence Metadata Activities*.
- This is the third report produced from the CSE Commissioner's broad review of CSE's use of metadata that began in 2013. This report presents the CSE Commissioner's findings on the portion of the review covering metadata activities in an information technology (IT) security context.
-
-

Background

- You received a letter from the CSE Commissioner, dated 5 December 2016, providing the results of his *Review of CSE Cyber Defence Metadata Activities*.
- This is the third report produced from the CSE Commissioner's broad review of CSE's use of metadata that began in 2013. This report presents the CSE Commissioner's findings on the portion of the review covering metadata activities in an information technology (IT) security context.

Considerations

Next Steps

- Attached is a proposed package for your consideration and response to the CSE Commissioner.

Greta Bossenmaier
Chief

Communications Security Establishment Commissioner

The Honourable Jean - Pierre Plouffe, C.D.

Commissaire du Centre de la sécurité des télécommunications

L'honorable Jean - Pierre Plouffe, C.D.

TOP SECRET//SI//CEO

Our file # 2200–101

December 5, 2016

The Honourable Harjit S. Sajjan, PC, OMM, MSM, CD, MP
Minister of National Defence
101 Colonel By Drive
Ottawa, ON K1A 0K2

Subject: Review of CSE Cyber Defence Metadata Activities

Dear Minister:

The purpose of this letter is to provide you with the results of a review of Communications Security Establishment (CSE) cyber defence metadata activities. I examined CSE use of metadata in an information technology (IT) security context to determine whether it complies with the law and does not direct its cyber defence activities at Canadians or any person in Canada and that it effectively applies satisfactory measures to protect Canadians' privacy. This review is the third and last in a series of recent investigations focused on metadata; the first two parts — submitted in 2015 and March 2016 — addressed foreign signals intelligence metadata activities.

The review was conducted under the Commissioner's general authority set out in paragraph 273.63(2)(*a*) of the *National Defence Act* (NDA) and the authority set out in subsection 273.65(8) of the NDA to determine whether activities carried out under a ministerial authorization (MA) are authorized by the Minister of National Defence. The review was led by a computer engineer and IT security expert contractor with 30 years' experience in the public and private sector, which provided the office with a new perspective on the activities. He examined CSE operational policy and procedures, received technical briefings and demonstrations, and conducted interviews.

CSE conducts cyber defence metadata activities under the authority of paragraph 273.64(1)(*b*) of the NDA and cyber defence MAs. The 2011 ministerial directive on metadata defines metadata as "information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its content." CSE may acquire cyber defence metadata from its own sources, from domestic and international partners, and from owners of computer systems of importance to the Government of Canada (GC).

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
T: 613-992-3044 F: 613-992-4096

s.26

Metadata remains essential to CSE's cyber defence mandate, for example, to identify and mitigate sophisticated foreign malicious cyber threats to help protect computer systems of importance to the GC. Past reviews on cyber defence activities conducted under MAs (recently, reports # 2200–104 in 2016 and # 2200–84 in 2015) and not conducted under MAs (report # 2200–69 in 2013) contain detailed background information, including on CSE acquisition and use of metadata for cyber defence activities. The reports and the office's working file also contain specific information on the systems, databases and tools used by CSE to, for example, analyze and retain metadata for cyber defence activities. I will not repeat background information in this letter; however, the following general points are worth noting.

CSE cyber threat detection capabilities copy and store a sub-set of GC client network data — including metadata — to identify and permit ongoing analysis of anomalous and sophisticated foreign malicious cyber events. CSE acquires only a small proportion of the data passing through its cyber defence sensors. CSE extracts metadata from the data acquired and uses it, for example, to contextualize the threat and malware and to develop mitigation advice for the client and other GC institutions.

CSE does not collect unselected (bulk) metadata under part (b) of its mandate (the 2015 review report addressed CSE collection of unselected metadata for the purpose of foreign intelligence under part (a) of its mandate); cyber defence activities acquire from GC networks both content and metadata relating to cyber events.

It is to be expected that CSE cyber defence activities may involve metadata relating to Canadians because the activities involve data from Canadian networks located in Canada — acquired either by CSE under an MA, or by system owners and GC institutions under *Criminal Code* and *Financial Administration Act* authorities and subsequently disclosed to CSE.

CSE cyber defence activities generally acquire communications containing nothing more than malicious code or an element of "social engineering" sent to a computer system in order to deceive the recipient and compromise the system.

Even so, CSE treats cyber defence metadata that could identify a communicant or the communication — for example, the "from" and "to" fields of an e-mail, or an Internet Protocol address linked to the communication — like a private communication (PC) and applies the same privacy protection measures to that metadata as it would to a PC.

Before this letter was finalized, CSE officials had an opportunity to review it for factual accuracy and to comment on the findings.

If you have any questions or comments, I will be pleased to discuss them with you at your convenience.

Yours sincerely,

Jean-Pierre Plouffe

cc: Ms. Greta Bossenmaier, Chief, CSE

Minister
of National Defence

Ministre
de la Défense nationale

Ottawa, Canada K1A 0K2

SECRET
CERRID # 32825877

FEV
FEB 21 2017

The Honourable Jean-Pierre Plouffe
Communications Security Establishment Commissioner
90 Sparks Street, Suite 730
P.O. Box 1984, Station B
Ottawa, Ontario, K1P 5B4

Dear Commissioner Plouffe:

I am writing to respond to your report dated 5 December 2016, entitled *Review of CSE Cyber Defence Metadata Activities.*

I read with interest your findings concerning CSE's metadata activities in an information technology (IT) security context, which marks the completion of your Office's three-part review of CSE's activities involving metadata that began in 2013.

Thank you for your report.

Sincerely,

The Hon. Harjit S. Sajjan, PC, OMM, MSM, CD, MP

cc: Greta Bossenmaier, Chief, CSE

PUBLIC OPINION RESEARCH INDIVIDUAL PLAN

This Public Opinion Research (POR) Individual Project Planning Template is intended to facilitate information sharing for projects requiring Deputy Head approval. The template is for both **contracted POR** and **significant non-contracted POR**[1] that is to be conducted with internal resources. Please refer to the Directive on the Management of Communications for more information.

Draft plans must be sent to the two following organizations before requesting Deputy Head approval:

- the Communications and Consultations Secretariat at Privy Council Office (PCO)
- the Public Opinion Research Directorate at Public Services and Procurement Canada (PSPC)

Once a plan has been reviewed and approved by the Deputy Head, an electronic version of the signed copy should be sent to your advisors at PCO and PSPC.

For assistance or advice at any stage of your project, please contact the Public Opinion Research Directorate (PORD).

Summary Public Opinion Research Project

Project Title	Attitudes Towards the Communications Security Establishment (CSE)
Project Overview and Research Objectives	As the first Public Opinion Research project ever undertaken by the CSE, this research project is intended to establish a baseline measurement of knowledge, attitudes and behaviours of Canadians with respected to the CSE, both in terms of its mandate and activities, and in terms of recruitment initiatives.
Information Needs	Information needs are as follows: - Establish a baseline measurement of views towards CSE in order to help measure the success of future communications initiatives. - Better understand the public's awareness and attitudes towards CSE to help shape communications strategies. - Explore awareness and views of career opportunities to help guide recruiting marketing strategies.
Rationale and Intended Use of Research[2]	The results of this research will be used to: - Shape communications strategies, and provide a baseline measurement to help measure their success. - Shape recruitment marketing strategies, and provide a baseline measurement to help measure their success.
Target Audience	All Canadians; over sample of technical professionals (science, technology, engineering and math).
Proposed Methodology	Random digit dialing telephone survey
Projected Timeframe	Contracted by Feb-17. Fieldwork completed by 31-Mar-17. Report in Apr-17
Single or Multi-year Project	Single year project. Separate tracking studies may follow.
Use of Internal Resources (Y/N)	Project will be contracted.
Partnerships and Resources Involved	Results will be shared with CSIS
Maximum Budget (including taxes)	$84,750 (including HST)

Department / Agency Name – Fiscal Year Date: _____

s.15(1) - DEF

Contact Information:

Deputy Head	Greta Bossenmaier, Chief, Communications Security Establishment
Head of Communications	**Dominic Rochon** Deputy Chief, Policy and Communications
Public Opinion Research Departmental Coordinator	Anda Carabineau
Project manager	

Recommended By:

D. Rochon — Jan 20/2017

Head of Communications — Date

Approved By:

A.S. — Feb 6th, 2017

Deputy Head — Date

[1] As per the Directive on the Management of Communications a public opinion research is deemed to be significant when the project:

- supports legislation, regulations or litigation;
- supports government or departmental priorities;
- addresses the development of new government policies, programs, services or initiatives;
- touches on issues that are of high public interest or sensitivity; or
- relates to any other important of high risk issue.

[2] **Rationale and Intended Use of Research** include a clear statement of the need for undertaking the projects against criteria developed by the Treasury Board of Canada Secretariat. It should include information on the:

- Manner in which research is prescribed by legislative, policy, evaluation or litigation requirement
- Manner in which research supports government or departmental priorities
- Manner in which research findings will benefit Canadians
- Alternate approaches and information sources considered and reasons for their unsuitability
- Risks associated with information gathering and dissemination
- Risks associated with failure to secure information

SECRET

FEB 03 2017

CERRID # 33143613

MEMORANDUM FOR THE MINISTER OF NATIONAL DEFENCE

Response to CSE Commissioner's

Review of the CSE Procedural Errors and CSE and Second Party Privacy Incidents

(For Approval)

Summary

- The CSE Commissioner completed his annual *Review of the CSE Procedural Errors and CSE and Second Party Privacy Incidents*.
-
-

BACKGROUND

- You received a letter and report from the CSE Commissioner, dated January 6, 2017, providing the results of his *Review of the CSE Procedural Errors and CSE and Second Party Privacy Incidents*.
- The review examined the process that CSE uses to monitor compliance of its operations with legal responsibilities, ministerial requirements, operational policies and procedures. The process involves compliance incidents and procedural errors of privacy interest, and the associated mitigative and corrective actions.
- The review examined three files including CSE Privacy Incident File (PIF), Second Party Incidents File (SPIF) and Minor Procedural Errors Record (MPER). The SPIF was introduced in January 2016 to clarify the record keeping process in relation to incidents attributable to CSE from those attributable to Second Party partners.
-

CONSIDERATIONS

- This review examined incidents recorded in the first six months of 2016, as well as two incidents that remained outstanding from late 2015.
-
-
-

NEXT STEPS

- Enclosed is a package for your consideration and response to the CSE Commissioner.

Greta Bossenmaier
Chief

TOP SECRET//SI//CEO

Our file # 2200–109

January 6, 2017

The Honourable Harjit Sajjan, PC, OMM, MSM, CD, MP
Minister of National Defence
101 Colonel By Drive
Ottawa, ON K1A 0K2

Subject: Review of CSE Procedural Errors and CSE and Second Party Privacy Incidents

Dear Minister:

The purpose of this letter is to provide you with the results of the most recent review of the Communications Security Establishment (CSE) Minor Procedural Errors File (MPEF), Privacy Incidents File (PIF), and new Second Party Incidents File (SPIF), which was implemented on January 1, 2016. The review was undertaken under the Commissioner's general authority articulated in Part V.1, paragraph 273.63(2)(*a*) of the *National Defence Act* (NDA).

Based on the review of the MPEF, PIF and SPIF records, CSE's answers to questions, and an independent verification of information in CSE databases,

Background

CSE policy OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities* (December 1, 2012), requires CSE foreign signals intelligence and information technology security employees to report and document privacy incidents. CSE reports and tracks privacy incidents and procedural errors, and the associated mitigative and corrective actions, as one measure to promote compliance with legal and ministerial requirements and operational policies and procedures, and to enhance the protection of the privacy of Canadians.

CSE examines compliance incidents to determine whether internal or external recipients were exposed to sensitive personal information of Canadians without appropriate authorization, and whether the incidents could result in potential harm to the Canadians. The PIF is a record of incidents attributable to CSE involving activities conducted in a manner counter to CSE operational policy and privacy guidelines and information being exposed to external stakeholders who ought not to have received it. The SPIF is a record of similar compliance incidents attributable to second party partners. These incidents may be identified by the partners themselves, or by CSE. The MPEF is a record of incidents where the information was contained within CSE and not exposed to external recipients.

Treasury Board of Canada Secretariat (TBS) makes a further distinction, defining a material privacy breach as a breach that "involves sensitive personal information and could reasonably be expected to cause serious injury or harm to the individual and/or involves a large number of affected individuals" (*Guidelines for Privacy Breaches*, section 4, May 5, 2014).

During the year, the Commissioner's office examines privacy incidents as part of separate, in-depth reviews of CSE activities, including the associated entries in the PIF and SPIF. However, individual reviews may not capture all incidents and CSE's response might be pending when an individual review report is issued.

The annual review of the MPEF, PIF and, as of this year, SPIF, focuses on incidents not examined in detail in the course of other reviews. It permits the identification of trends or systemic weaknesses that might suggest a need for corrective action, changes to CSE's procedures or policies, or an in-depth review of a specific incident or activity. For example, the office could investigate an incident identified by CSE as a material privacy breach or could examine an incident to determine whether it was a material privacy breach.

The objectives of the review were to:

- acquire knowledge of the procedural errors, incidents and subsequent actions taken by CSE to correct the incidents or mitigate the consequences;
- acquire knowledge of any CSE operational material privacy breaches and CSE's associated corrective actions;
- determine what incidents, if any, may raise questions about compliance with the law or the protection of the privacy of Canadians; and
- help evaluate CSE's policy compliance validation framework and monitoring activities.

Methodology

The review is based on an examination of the MPEF, PIF and SPIF records for the period, CSE's answers to questions, and an independent verification by the office of reports in — which is CSE's database of end-product reports — as well as Canadian entities designated as Protected in which is CSE's target information database.

Findings

MPEF

in the MPEF noted a discovery that an analyst's account folder, which was linked to a "raw" (i.e., unassessed) data repository, contained files dating from that may have contained private communications and that had not been deleted in accordance with CSE's retention schedule. According to CSE, the folder was subsequently deleted without any of its files having been opened, and CSE undertook to routinely review and delete the data in that repository.

other entries involved Canadian Identity Information (CII) being made available to one or more unintended recipients within CSE due to technical issues and/or human error; technical solutions were implemented to prevent reoccurrences. involved having potential unintended access to ; however, according to CSE officials, access logs confirmed that only authorized persons actually viewed the data. consisted of the inadvertent inclusion of a Canadian identity in an end-product report; however, based on CSE information, audit logs confirmed that only CSE employees — specifically the report's two authors and two CSE Client Relations Officers — had accessed the report before it was cancelled.

PIF and SPIF

A total of 55 privacy incidents were reported in the six-month period under review — attributable to CSE (PIF) and to its second party partners (SPIF).

Of the incidents attributable to CSE, involved the inadvertent sharing or inclusion in a report of CII without suppressing the information in accordance with CSE naming policies. In all but one of these incidents, it was unknown at the time the reports were issued that the information pertained to a Canadian or a person in Canada. The remaining incident was due to human error and was quickly rectified. In all instances, the reports were cancelled or corrected with the identities properly suppressed. In incidents, the nationality of the Canadian was known within certain areas of CSE, that is, specifically

incidents also involved the sharing within CSE of CII obtained from reporting that should have had a very limited distribution within CSE given the sensitivity of the information.

The remaining incidents involved unintentional targeting or database searches for information relating to individuals not previously known to be Canadian or persons in Canada. In several of these incidents, the incidents involved a foreign intelligence target One instance involved a targeting incident in support to a request for assistance from under part (c) of CSE's mandate, before receiving all required authorizations from CSE senior management. In all of these instances, CSE deleted any associated intercepted communications or reporting.

Of the privacy incidents attributable to the Second Parties, involved the inclusion in a report of CII of individuals not previously known to be Canadian or persons in Canada. Another incident involved a report that mistakenly labelled a Canadian as a national of a second party country. While the Canadian was not identified in the report, it is uncertain whether, as a consequence of the mislabeling, the Canadian's identity might have been subsequently shared by second party partners with their clients without the express permission of CSE. The final incident consisted of a Canadian permanent resident having been named in a total of reports issued by second party partners during the period. In when CSE authorities became aware that these reports existed, a report cancellation request was issued to agencies; however, owing to the age of the reports, the report cancellations, which were carried out by the originating agencies, did not automatically result in the reports being deleted from as they normally would. When it was discovered, months later, that the reports still resided in CSE manually purged them from the system.

As part of the review, office employees reviewed end-product reports in that were referenced in the SPIF. They discovered that of the second party reports contained an belonging to a Canadian, even though both reports had been reissued with the CII suppressed and CSE had received confirmation by the issuing second party partner that the original reports had been cancelled. As a follow-up to the office's inquiry, CSE manually purged these reports from It is not clear why the reports had not been deleted from automatically upon their cancellation, as expected.

The Deputy Chief, Policy and Communications, is CSE's Chief Privacy Officer, and is responsible for determining, in consultation with the Department of Justice Canada, if an incident constitutes a material privacy breach. Such determination is guided by the TBS diagnostic tools relating to material privacy breaches and CSE's internal policies and procedures. CSE did not identify any operational material privacy breach as having occurred during the period under review.

General observations and opportunities to enhance privacy protection

Since the previous review, CSE issued PCI-4, *Handling Operational Compliance Incidents*, a new policy instrument setting out the procedures for CSE employees to follow in handling privacy incidents and procedural errors. CSE quickly corrected minor inconsistencies in the policy identified by the office.

Before this letter was finalized, CSE officials had an opportunity to review it for factual accuracy and to comment on the findings.

If you have any questions or comments, I will be pleased to discuss them with you at your convenience.

Yours sincerely,

Jean-Pierre Plouffe

cc: Ms. Greta Bossenmaier, Chief, CSE

Minister
of National Defence

Ministre
de la Défense nationale

Ottawa, Canada K1A 0K2

SECRET
CERRID # 33183524

FEV
FEB 21 2017

The Honourable Jean-Pierre Plouffe
Communications Security Establishment Commissioner
90 Sparks Street, Suite 730
P.O. Box 1984, Station B
Ottawa, Ontario, K1P 5B4

Dear Commissioner Plouffe:

I am writing to respond to your report dated 6 January 2017, entitled *Review of the CSE Procedural Errors and CSE and Second Party Privacy Incidents*.

Thank you for advising me of the results of this review.

Sincerely,

The Hon. Harjit S. Sajjan, PC, OMM, MSM, CD, MP

cc: Greta Bossenmaier, Chief, CSE

Canada